ISSN No:-2456-2165

The Emergence of Blockchain Technology: A Practical and Secure Approach

Mikhil Chohda

Abstract:- This study aims to explore Blockchain technology which is a new technology that has the potential to alter many sectors by making procedures more democratic, safe, transparent, and efficient. Blockchain technology's broad adoption has had a significant influence on how people deal in the digital world. The use of blockchain technology has been expanding across a number of industries as technology advances. Blockchain is an emerging technology that enables smart contracts to perform a variety of processes and different jobs. The foundation of blockchain is smart contracts, which have the ability to replace the position of "middle man" as it can reduce costs, minimize delays, offer more timely and precise data, and improve reporting accuracy. This makes it incredibly difficult for hackers to change or breach blockchain data, especially in a system using a public blockchain. PoC Design is the name given to the new IoT-PoC development process based on extreme programming.

Keywords:- *Blockchain, types of blockchain, Transformation of the financial industry, smart contracts, blockchain, and real business value.*

I. INTRODUCTION

Encryption and dissemination are the foundations of the relatively new technology known as blockchain. All committed transactions are recorded in a series of blocks, which may be thought of as a public ledger for the blockchain. This chain expands as additional blocks are consistently added to it. The peer-to-peer architecture of the blockchain enables each node to share an updated ledger through peer-to-peer replication, where all transaction information are transferred onto each node. Each node has the ability to transmit and receive transactions to other nodes, and local data is constantly updated with the global datasheet.

Bitcoin and other forms of decentralized digital currency were among the first implementations of blockchain technology in the financial sector. The use of blockchain is expanding across a number of industries as technology advances. Blockchain is transforming a number of business applications because to its intriguing advantages, like trust, and no exchange transaction cost. Although many financial and non-financial players are enthusiastic potential of this technology, a question that occupies the industryLeaders: How to Spot a Good Blockchain Business Case?

Financial traders are the first to embrace this technology, although it is still in its infancy. Investigations of the World Economic Forum1 predict that banks and regulators around the world will be ready to experiment with different blockchain prototypes in 2017. With more than 90 central banks involved in the global blockchain discussion, more than 2,500 patents have been filed in the last three years. Blockchain technology is years old and expects 80% of banks to launch blockchain and distributed ledger technology (DLT) projects by 2017. It is on the way to becoming the new normal in the world of financial services.

II. BLOCKCHAIN IN DETAIL

A. Blockchain Architecture

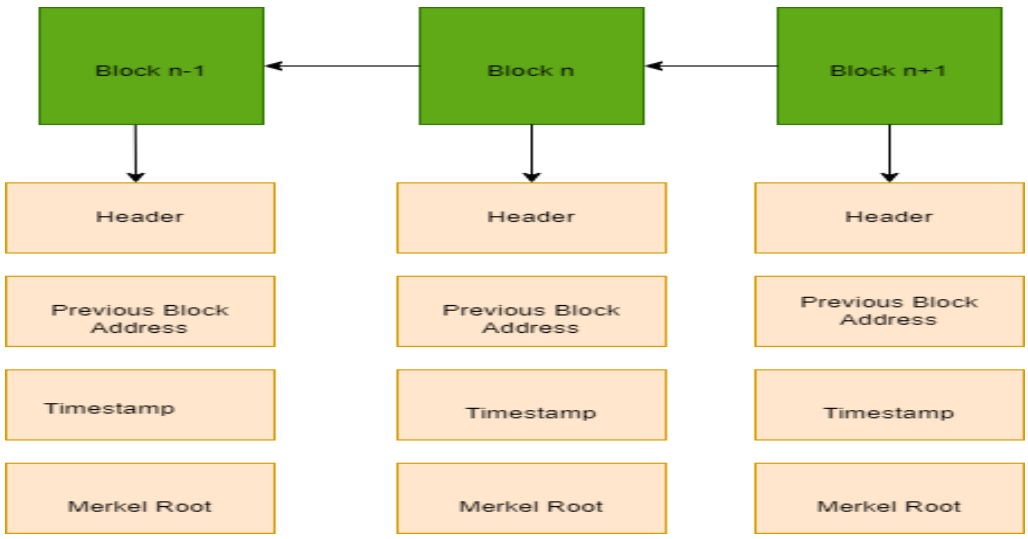

Fig. 1: An example of a blockchain consists of a continuous sequence of blocks.

ISSN No:-2456-2165

- **Header:** A block header identifies the specific block on a blockchain and is hashed repeatedly to generate proof of work for mining rewards. A blockchain is made up of numerous blocks that are used to record information about transactions that take place on the blockchain network.
- **Previous Block Address**: The header of each block in the blockchain contains a hash that was created using the SHA256 cryptographic hash technique. The "previous block hash" feature in the block header allows each block to refer to a preceding block, often known as the parent block.
- **Timestamp:** It is a system that examines block data and assigns a creation time or date to digital documents. A timestamp is a string of characters that uniquely identifies a document or event and indicates when it was created.
- **Nonce:** A nonce is a random number that is added to a block of data before it is encrypted in the context of the blockchain. Miners use this attribute to validate transactions and create new blocks since enabling nonce changes the hash of the data. It ensures that the hash of the block is unique and discourages attackers from altering the blockchain since it is only used once.
- **Merkel Root:** It is a kind of data structure frame that consists of different data blocks. The Merkle root is a simple mathematical method of confirming the Merkle tree facts. They are used in cryptocurrencies to ensure blocks of data sent over a peer-to-peer network are complete, intact and unaltered.

B. Features of Blockchain Architecture

- **Decentralization:** The entire distributed database is available to every participant of the blockchain structure. Compared to centralized systems, consensus algorithms allow network control.
- **Anonymity:** Each participant in the blockchain network has a unique address, not a user ID. This protects user privacy, especially in a system using a public blockchain.
- **Cryptography:** All blocks on the blockchain network strive to be safe since the blockchain idea is entirely focused on security. Additionally, it employs cryptography for security and encrypts the data using ciphers.
- **Transparency:** Fraud cannot enter the blockchain system. Because it would require a lot of processing power to completely replace the blockchain network, this is very unlikely to happen.
- **Persistence**: Transactions can be confirmed fast, and users or cryptocurrency miners would not accept any incorrect transactions. Once a transaction is a part of the blockchain network, it cannot be deleted or rolled back. Transactions that are invalid are not carried on.

C. Type of Blockchain

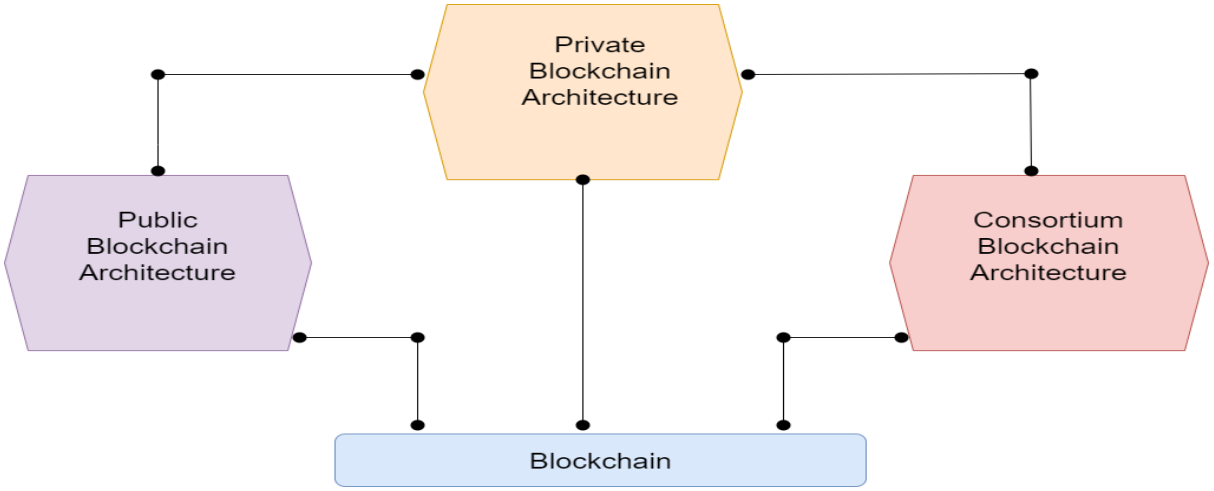

Fig. 2: Type of blockchain

➢ *Public Blockchain*

The public blockchain runs in an open environment or over a large network of nodes, with users using anonymous identities and having open read/write access to the database. The first public blockchain was Bitcoin, which was rapidly followed by the equally popular Ethereum. Traditionally, the Pow (Proof-of-work) consensus technique was utilized; however, several block chains have included newer alternatives such as PoS (Proof-of-stake). The business sector, on the other hand, is disinterested in public blockchain since its characteristics such as anonymous identity, publicly accessible data, and unlawful access do not suit industrial use cases. [1] (2019, A Study of Emerging Areas in Blockchain Adoption and Prospective Challenges in India)

➢ *Private Blockchain*

Blockchain technology's broad adoption has had a significant influence on how people deal in the digital world. Individuals can deal anonymously but transparently. Their names are concealed, but the records of their transactions are public. This offers advantages in some applications, but it may not be appropriate for transactions when it is critical to know who you are dealing with or where the data on the blockchain is confidential. Because only authorized users may transact on the network, private blockchain networks are more suited for such transactions. Sensitive data can also be maintained on the blockchain since the people who can access the specifics of the transactions can be limited [2] (Ncube et al., 2020).

ISSN No:-2456-2165

➢ *Consortium Blockchain*

A consortium blockchain is a form of blockchain network that is controlled by a small number of businesses rather than being available to the public like a permissionless or public blockchain. This consortium of organizations collaborates to validate and add transactions to the blockchain in order to ensure the network's integrity and security.[1] (*A Study of Emerging Areas in Adoption of Blockchain Technology and It's Prospective Challenges in India*, 2019)

Table 1: Comparisons among public blockchain, consortium blockchain and private blockchain

Property	**Public blockchain**	**Private blockchain**	**Consortium Blockchain**
Transaction speed	Slow	Lighter and faster	Lighter and faster
Centralized	No	Yes	Partial
Access	Anyone	Single Organization	Multiple selected organization
Security	consensus mechanism	Pre-approved participants	Voting/multi-party consensus
Consensus Process	Permissionless	Permissioned	Permissioned

III. TRANSFORMATION OF THE FINANCIAL INDUSTRY THROUGH BLOCKCHAIN

- Asset Management: The ability of distributed ledgers to replace the role of "middle man" has had a considerable impact on buy-side firms, with the potential to reduce costs, shorten delays, provide more accurate and exact data, and increase reporting accuracy. Blockchain has the potential to have a significant impact on the agreement of securities transactions and give a significant opportunity to reduce asset managers' expenses, resulting in cheaper charges for shareholders.Each trader is comprised of broker dealers, intermediaries, custodians, clearing and settlement teams, and they preserve a record of all transactions. Blockchain technology allows for an automated trade lifecycle in which all parties involved have access to the transaction. [3] Mathew and Quadir (2018)
- Digital banking: Banking and client relationships will continue to be prioritized (Mekinji, 2019) [14]. Meanwhile, with a range of digital banking solutions, digital banking platforms provide users with access to all online banking services (North, 2020) [15].The adoption of digital technology has compelled traditional banks and other financial institutions, who have traditionally been on the front lines, to modernize their operations. Iman (2019) [16] defines talents and knowledge.
- Supply Chain: Smart contracts are automatically performed on the blockchain to transfer titles of goods and money, creating a trusted network of ensured authenticity and the origin of products provided.

Table 2: Blockchain Transformation of Financial Services [5] (Table 1 . Blockchain Transformation of Financial Services, n.d.)

Function	**Blockchain impact**	**Stakeholders**
Authenticating Identity and Value	Verifiable and robust identities, cryptographically assured	Rating agencies, consumer data analytics, marketing, retail banking, payment card networks regulators
Exchanging Value	Enhancing speed dramatically	All industries
Funding and Investing	New models	Investment banking, venture capital, legal, audit, property management, stock, exchange, regulators
Management Risk	Lowering risk	Insurance ,risk management, wholesale banking, brokerage, clearinghouses, regulators
Accounting for value	Dramatically improved reporting	Audit, accounting, regulators

IV. SMART CONTRACT IN BLOCKCHAIN

The phrase "smart contracts," also known as "self-executing contracts," "blockchain contracts," or "digital contracts," refers to a digitalized ledger that may be converted to computer code and maintained, replicated, and monitored by the blockchain network of nodes. The decentralized ledger also stores and copies the document, providing security and immutability. A smart contract approach involves moving an asset or currency into a program "and the program runs this code and at some point, it automatically validates a condition and naturally determines whether the asset should be transferred to one person or returned to the other, or whether it should be immediately reimbursed to the person who sent it." Contracts that are smart Smart contracts pave the path for business and distributed ledger technologies by ensuring autonomy, trust, backup, safety, speed, savings, and accuracy. It assures that there will be no doubt and that there will never be a need for litigation, resulting in a highly exact set of results. Smart contracts, which can execute a range of operations and functions, are the core of blockchain technology. [4] Quadir and Mathew (2018).

ISSN No:-2456-2165

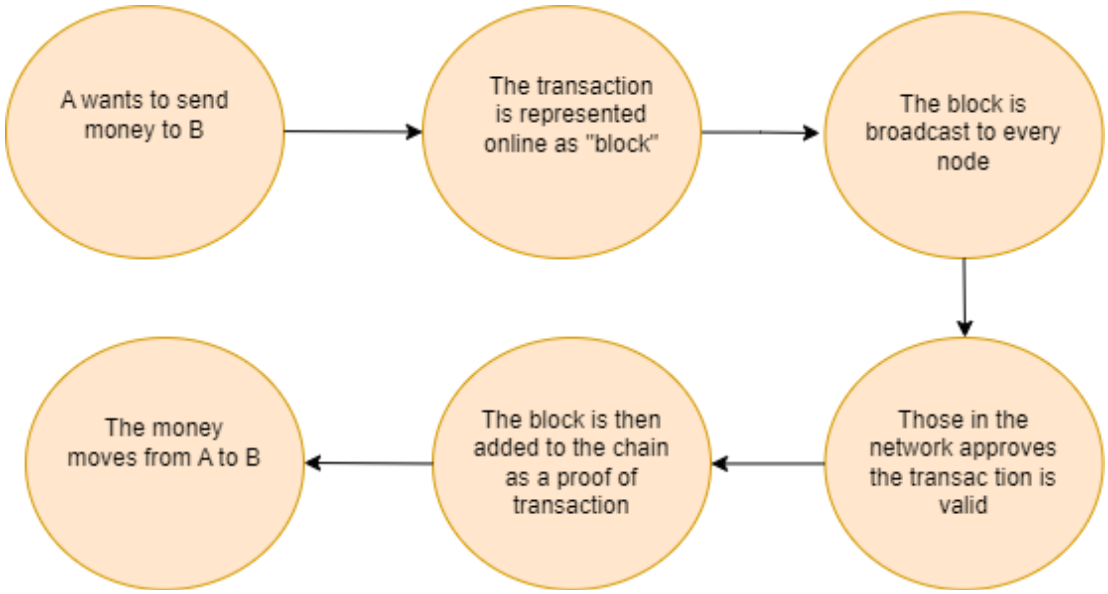

Fig. 4: Workflow of blockchain mining.

V. BLOCKCHAIN & ACTUAL BUSINESS VALUE

Blockchain is a new technology that has the potential to alter many sectors by making procedures more democratic, safe, transparent, and efficient. Blockchain 3.0, which delivers increased interoperability, scalability, and security, is becoming popular.This opens the door for blockchain to grow and provide real corporate value.

A. The Value Proposition

The blockchain has attracted a lot of attention because of the value that it offers. The three key pillars of Blockchain Technology that have contributed to its global acceptance are as follows:

- **Transparency and immutability**: Blockchain provides a transaction record that is both transparent and immutable. Once a transaction has been recorded on the blockchain, it cannot be readily edited or tampered with. This capability assures the integrity and validity of data, making it perfect for high-trust applications like financial transactions or supply chain management.[6] (Viriyasitavat & Hoonsopon, 2019).
- **Security**: To safeguard data and transactions, blockchain employs powerful cryptography algorithms. Each transaction is confirmed and connected to the one before it using a cryptographic hash, producing a block chain. This makes it incredibly difficult for hackers to change or breach the blockchain data.
- **Potential Applications**: Blockchain has the potential to transform sectors other than banking. It has applications in supply chain management, healthcare, voting systems, identity verification, intellectual property protection, and other areas. Its adaptability and potential to disrupt existing systems have sparked considerable interest and enthusiasm. [6] (Viriyasitavat & Hoonsopon, 2019).

VI. DEVELOPMENT AND IMPLEMENTATION PROCESS OF A BLOCKCHAIN

Current blockchain initiatives are divided into three stages: proof-of-concept (POC), minimum viable product (MVP), prototype development, and alpha/beta testing.

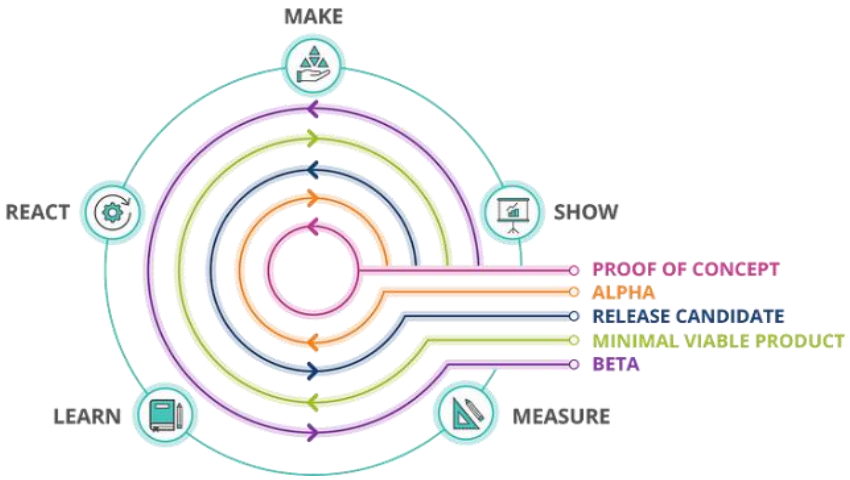

Fig. 5: Stages of product prototyping

ISSN No:-2456-2165

- **Proof of Concept (PoC):** Proof of Concept(PoC) The new IoT- PoC development methodology was designed grounded on extreme programming and has been named PoC Design. Its main goal is to enhance IoT- PoC development. With enhancement, the number of successful IoT systems may increase. The methodology is grounded on clarifying a problem or need. The key is to break the problem or satisfy the need. A result that doesn't give marketable value to the client shouldn't be developed but should be snappily rejected, and new results should be developed. The result, which is considered to have the stylish eventuality and capacity, is used in the development phase. As a result, no PoC is developed that isn't embedded in a problem, need, or business advantage. The idea is that no coffers should be spent on results that don't induce enough value in return(5)(Maddikunta etal., 2020)

- **Minimum Viable Product (MVP)**: Baseline data must be collected in order to assess the impact of the MVP. Additional data will be gathered as part of scheduled tests on the initial MVP and its succeeding versions. The amount and complexity of examinations can be mind-boggling. In an online consumer business, the number of distinct versions of a product performing various tests might number in the hundreds and vary every week, if not daily.

  Regardless of how difficult it is to manage that complexity, the more important topic is how to establish what needs to be tested in order to assess the impact of these tests. To overcome this issue, Ries proposes considering three sorts of growth engines: sticky, viral, and paid. (MVP Explained: A Systematic Mapping Study on the Definitions of Minimal Viable Product, n.d.) [8]

- **Alpha and Beta Testing:** The findings of the alpha test, which included content specialists, showed that the prototype matched the learning needs related with the Nutrition topic. In terms of the Malaysian Ministry of Education (MOE) Science syllabus, the material of this prototype was correct, complete, and current. Content specialists also discovered that the narrator's voice quality was good and matched the quality of the animated video presentation that had been created. Beta testing comes after revisions and uses the entire product for testing. Students and Science professors participated in the beta test. This is the official procedure for determining the prototype's usability. The beta test was carried out as a practice run before the actual test. It also informs the researcher about any unanticipated difficulties that may develop as a result of using the computer or the courseware's contents. (Personalized Learning Environment: Alpha Testing, Beta Testing & User Acceptance Test, 2015)[9]

VII. ECENTRALIZED IDENTITY AUTHENTICATION

In contrast to centralized identity management systems, such as Microsoft's Active Directory, in which third parties maintain and modify identities, decentralized identity (DID) is an identification system in which identity information is controlled by the entity that produces it. Today, most DIDs employ blockchains to maintain a mapping between a unique identifier (representing an entity) and additional metadata, such as cryptographic keys.

The advantages of DIDs are directly drawn from those of blockchains—the (did, meta) tuples are tamper-evident and widely available. Furthermore, DIDs may ensure that only the original owner of a registered did can edit the accompanying information, providing the user complete control over their identity (Alangot et al., 2022). [10]

A. Privacy Issues in a Decentralized System

- A blockchain is a public ledger that makes all information available to everyone. If a person's personal information is compromised during a transaction, all of their transactional information is at risk. This could lead to the revealing of sensitive information. This is how much money people spend (Hassan et al., 2019).[12]
- Decentralization is expected to address offline privacy concerns because data is no longer gathered and owned by a single logical entity. However, data distribution among peers in a decentralized network presents a new threat model with complex technological hurdles, particularly when it comes to managing online privacy. That is, access control and rights management become the shared duty of the several peers who keep a user's data. As a result, one of the new essential jobs is coordination and consensus agreement to preserve the system's secure state.(Bahri, Carminati, & Ferrari, 2018c) [19]
- Users in existing DID systems are unable to detect credential misuse when user credentials are hacked (Alangot et al., 2022). It also addresses the issue of policing fraudulent accounts and material that may harm privacy. This is because fake accounts can build relationships with legitimate users, access their personal data, and are more difficult to detect and eliminate (Bahri et al., 2018b).

B. Various measures for privacy protection

- **Task confidentiality:** The most basic security criterion for establishing task security is task secrecy. The assignment is encrypted and uploaded to our system's cloud server platform, which is considered fascinating. In the worst-case situation, the cloud server platform may try to restore the task information but fail because it either lacks a secret key or the attribute does not fit the access rules. As a consequence, the system can safeguard the secrecy of the work. (2022) [11]
- **Decentration:** By utilizing blockchain, we can achieve end-to-end crowdsourced work management. Requesters and staff might engage directly during this procedure. It prevents DDoS assaults, single points of failure, and data leaking that may occur on a centralized administration platform. (2022) [11]
- **Distributed consensus algorithms:** In decentralized identity systems, distributed consensus algorithms are used to ensure that all nodes in the network agree on the system's state. This prevents tampering and ensures the data's integrity (Kovalchuk et al., 1970).

ISSN No:-2456-2165

VIII. RESEARCH METHODOLOGY

I reviewed existing research papers and articles on Google Scholar in depth. This aided me in developing a fundamental understanding of blockchain technology, including its history, current advancements, and emerging trends. I used this review to identify knowledge gaps and develop research topics. Academic papers and articles collected on Google Scholar served as my major data source. These papers were authored by industry specialists and provided significant insights into various elements of blockchain. To ensure a thorough perspective, I supplemented my main data with information from reliable sources such as industry papers and websites. I read and evaluated the study papers thoroughly, obtaining critical information on blockchain kinds, financial applications, architectural aspects, real-world commercial value, obstacles, and privacy measures. This analysis provided me with a better knowledge of each sub-topic. I used real-world case studies from research publications to demonstrate the practical applications of blockchain. These case studies demonstrated how blockchain is being used in fields such as cross-border payments, trade finance, and digital identity verification. Throughout my study, I made certain that the sources I used were properly mentioned and referenced, providing credit to the original writers. I also honored intellectual property rights by relying on reliable sources of information.

IX. RESULTS AND DISCUSSIONS

Many company models, digital identities, service platforms, and systems in today's society work in a centralized setting. It denotes that control and ownership are held by a single body or authority. This may be observed in different social media and e-commerce platforms where individuals have no control over their identity record, resulting in the leak and exploitation of their private data and information. As a result of these issues, decentralized identification solutions are necessary.

Blockchain improves the trustworthiness, security, openness, and traceability of data exchanged across a corporate network – while also delivering cost savings through new efficiencies. Blockchain for business employs a shared and immutable ledger that can only be viewed by those who have been granted access. Every transaction is recorded in a permanent and unchangeable record thanks to blockchain technology. Fraud, hacking, data theft, and information loss are all impossible with this unbreakable digital ledger.

The use of blockchain technology boosts trust in online transactions. Conversations while giving them greater control over their online appearance. The investigation focused on ensuring privacy in decentralized identifying methods and the issues associated. By reducing reliance on centralized authority, decentralized systems improve privacy. Because scalability and performance have become critical concerns, research may focus on enhancing the user experience of decentralized identity systems as well as understanding the components that influence user adoption. Decentralized identification systems are becoming increasingly popular.

X. CONCLUSION

Finally, this research paper has given a deep assessment of blockchain technology and its consequences in the banking world. We investigated the core notions of blockchain, such as its decentralized and immutable nature, as well as various blockchain topologies such as public, private, and consortium blockchains.

The study emphasized the true commercial value that blockchain delivers to numerous sections of the financial sector. Blockchain has the potential to transform financial services such as cross-border payments, trade financing, and supply chain management by improving transparency, traceability, and efficiency. Businesses may streamline processes, decrease expenses, and increase stakeholder confidence by embracing smart contracts and decentralized networks.

However, I have highlighted issues that must be solved before the full promise of blockchain technology can be realized. Scalability challenges, privacy concerns, and regulatory compliance are just a few of the major roadblocks that must be properly managed. Organizations must find a balance between the advantages of transparency and the preservation of sensitive information. To secure sensitive data and successfully address privacy issues, robust privacy protection techniques such as encryption, data obfuscation, and user permission processes must be employed.

Based on my findings, blockchain technology has the potential to revolutionise the financial industry and provide tremendous value to both firms and customers. To realize this promise, stakeholders must collaborate, develop, and strategically implement blockchain technologies. Before scaling up, organizations must do extensive Minimum Viable Product (MVP), proof-of-concept, alpha, and beta testing to prove the viability and utility of blockchain implementations.Before scaling up, organizations must do extensive Minimum Viable Product (MVP), proof-of-concept, alpha and beta testing to prove the viability and utility of blockchain implementations.

As blockchain technology evolves, more study is required to investigate new patterns, overcome technological limits, and investigate the social, legal, and ethical ramifications. Future research should look into how blockchain can be integrated with other revolutionary technologies like artificial intelligence, the internet of things, and decentralized finance.

In conclusion, the outcomes of this study demonstrate the transformational impact of blockchain technology in the financial industry. Organizations may uncover new prospects for creativity, efficiency, and trust by using its fundamental characteristics and tackling associated problems. Adopting blockchain technology while recognizing its promise and limits will be critical to flourishing in the increasingly digital and linked financial ecosystem.

ISSN No:-2456-2165

REFERENCES

[1.] A Study of Emerging Areas in Adoption of Blockchain Technology and It's Prospective Challenges in India | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9092935?denied

[2.] Ncube, T., Dlodlo, N., &Terzoli, A. (2020, November 25). *Private Blockchain Networks: A Solution for Data Privacy*. https://doi.org/10.1109/imitec50163.2020.9334132.

[3.] Mathew, S. A., & Quadir, A. (2018, January 1). *Evaluation of Blockchain in Capital Market Use-Cases*. International Journal of Web Portals; IGI Global. https://doi.org/10.4018/ijwp.2018010105.

[4.] Mathew, S. A., & Md, A. Q. (n.d.). *Evaluation of Blockchain in Capital Market Use-Cases.* Evaluation of Blockchain in Capital Market Use-Cases: Computer Science & IT Journal Article | IGI Global. https://doi.org/10.4018/IJWP.2018010105.

[5.] Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Blockchain-Transformation-of-Financial-Services_tbl1_324158510

[6.] Jani, S. (2019). The Emergence of Blockchain Technology & its Adoption in India. ResearchGate. https://doi.org/10.13140/RG.2.2.30997.58087

[7.] *Redirecting*. (n.d.). Redirecting. https://doi.org/10.1016/j.comcom.2020.05.020

[8.] MVP Explained: A Systematic Mapping Study on the Definitions of Minimal Viable Product. (n.d.). MVP Explained: A Systematic Mapping Study on the Definitions of Minimal Viable Product | IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7592786

[9.] *Personalized Learning Environment: Alpha Testing, Beta Testing & User Acceptance Test*. (2015, July 26). Personalized Learning Environment: Alpha Testing, Beta Testing & User Acceptance Test - ScienceDirect. https://doi.org/10.1016/j.sbspro.2015.06.319

[10.] Alangot, B., Szalachowski, P., Anh Dinh, T. T., Meftah, S., Gana, J. I., Mi Aung, K. M., & Li, Z. (2022, December 21). Decentralized Identity Authentication with Auditability and Privacy. MDPI. https://doi.org/10.3390/a16010004

[11.] H., Yang, K., Yang, B., Zhou, Y., Wang, T., & Gong, L. (2022, March 24). Privacy Protection of Task in Crowdsourcing: Policy-Hiding and Attribute Updating Attribute-Based Access Control Based on Blockchain. Privacy Protection of Task in Crowdsourcing: Policy-Hiding and Attribute Updating Attribute-Based Access Control Based on Blockchain. https://doi.org/10.1155/2022/7787866

[12.] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*, 512–529. https://doi.org/10.1016/j.future.2019.02.060

[13.] Kovalchuk, L., Oliynykov, R., Bespalov, Y., &Rodinko, M. (2022, April 4). Methods of Ensuring Privacy in a Decentralized Environment. Methods of Ensuring Privacy in a Decentralized Environment | SpringerLink. https://doi.org/10.1007/978-3-030-95161-0_1

[14.] Mekinjić, B. (2019). THE IMPACT OF INDUSTRY 4.0 ON THE TRANSFORMATION OF THE BANKING SECTOR. *Journal of Contemporary Economics*, *1*(1). https://doi.org/10.7251/joce1901006m

[15.] North, R. 2020. What is the impact of digital banking services in today's world? Enterprises Edge.

[16.] Iman, N. (2019). Traditional banks against fintech startups: a field investigation of a regional bank in Indonesia. *Banks and Bank Systems*, *14*(3), 20–33. https://doi.org/10.21511/bbs.14(3).2019.03

[17.] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: A comprehensive introduction," Princeton University Press, 2016.

[18.] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 2016.

[19.] Bahri, L., Carminati, B., & Ferrari, E. (2018b). Decentralized privacy preserving services for Online Social Networks. Online Social Networks and Media, 6, 18–25. https://doi.org/10.1016/j.osnem.2018.02.001

[20.] Bahri, L., Carminati, B., & Ferrari, E. (2018c). Decentralized privacy preserving services for Online Social Networks. *Online Social Networks and Media*, *6*, 18–25. https://doi.org/10.1016/j.osnem.2018.02.001